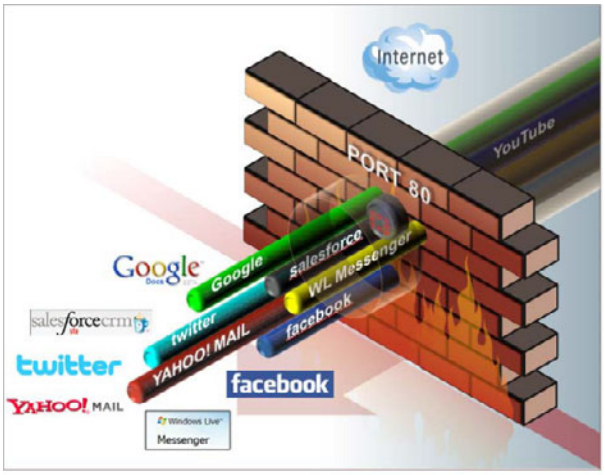
INSIDE FORTIOS

FORTINET

Application Control

FortiOS Application Control enhances content-based security by empowering you to monitor the applications that are on your network and take steps to control them

Monitoring and Controlling Applications, Not Just Network Ports



Controlling and monitoring applications on a network can seem like a daunting task because of the wide range of applications to be found. Blocking or allowing TCP and UDP ports that applications use is no longer an option since applications no longer map to individual ports. Web filtering can block individual sites but is not useful for complex social networking sites that might have some features of value. As well many applications just can't be blocked by web filtering.

Application control that complements content-based security is an essential part of a complete network protection solution. Technologies such as Web 2.0, social media, cloud computing, and virtualization have increased the complexity of network traffic and increased the need to understand what is happening on a network.

FortiOS Application Control

FortiOS Application Control uses efficient techniques to provide a visual picture of the applications that generate traffic on any network. Application control samples network traffic without affecting network performance. When application traffic is visible, all unwanted applications can be blocked and access control, traffic shaping, antivirus protection, antispyware protection, intrusion prevention, and other UTM features can be applied to the application traffic that is allowed. After applying control measures, ongoing monitoring continues to ensure that the measures are effective and to look for and manage changes in application traffic patterns.

Top Sessions by Application

Application	Sessions	Bytes (Sent/Received)
HTTP.Video	2	21.23 M
Dropbox	2	37.19 K
Youtube	2	26.71 K
LogMeIn	1	18.56 K
SSL	2	12.33 K
HTTP.BROWSER.Firefox	1	4.51 K
DNS	13	3.71 K

Effective application control starts with configuring application monitoring to get a picture of the application traffic on a network. FortiOS provides periodic and real-time Security Analysis reports by bandwidth and number of sessions that display the source and destination addresses of the application traffic.

Application control can be applied to regular network traffic and to IPsec and SSL VPN traffic terminated by the FortiGate unit as well as SSL-encrypted traffic including HTTPS, POP3S, SMTPS, and IMAPS passing through the FortiGate unit.

Application control can also be applied by the FortiOS Endpoint Control feature to monitor and control the applications that can be used by individual endpoints on your network. These endpoints include client computers and portable wireless devices connected to your network and running FortiClient. You can enforce endpoint application control by requiring end points to have FortiClient installed before they can get access through the FortiGate unit.

Application Control Sensors

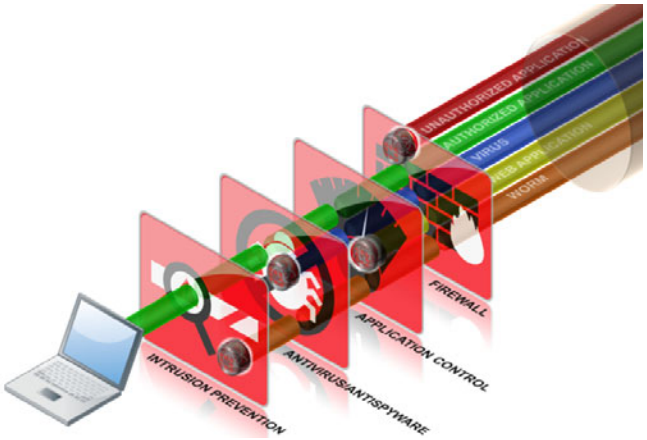
You can create multiple application control sensors, each configured to allow, block, or monitor a unique list of applications. In firewall policies that accept application traffic, you can enable application control and select an application control sensor. Traffic accepted by firewall policies is examined for the applications in the application control sensor, and the configured action is executed.

Application control sensors contain both filters and entries. Filters help to filter through specific application information such as the vendor of the application, the application's behavior, and the type of technology the application is, for example within a web browser. Entries help to monitor or block specific applications, or applications within applications. For example, you need to block Farmville, CuteBear and other non-productive applications within Facebook, but allow chat and playing videos.

Each application sensor also defines what action is taken with applications not included in the list. Unlisted applications can be blocked so that only traffic from listed applications can pass, effectively creating an application white list. The default behavior allows all unlisted applications, effectively creating an application black list where only the traffic from applications that you explicitly block is not allowed to pass. A locked down high-security network can use an application control list configured as a white list. A more open network that requires blocking of only a few applications can use a black list. You can also mix the white list and black list approach on the same network.

The FortiGuard Application Control Database

FortiOS application control detects more than 2,400 different Web-based applications, software programs, network services and network traffic protocols. FortiOS uses the FortiGuard Application Control Database, one of the largest application signature databases available. The database is constantly updated to recognize new applications and new versions of existing applications. Application control updates are downloaded to FortiGate units on demand, or as scheduled from the FortiGuard Distribution Network. FortiGuard push updates ensure that FortiGate units have up-to-the minute application databases.



A complete list and detailed information about all supported applications is available from the online FortiGuard Application Control Site. You can also go to the Application Control Updates page to see the latest additions to the database. You can use our Application Control Submission Form to request the addition of an application to the database.